

PureVPN's OpenVPN Setup Guide for pfSense (2.4.4)

pfSense is an open source firewall and router that is available completely free of cost. It offers load balancing, unified threat management, multi WAN, and other features for those particularly concerned about their online security and privacy.

Fortunately, users can further enhance its capabilities via PureVPN's OpenVPN, which can be setup on the latest pfSense (2.4.4).

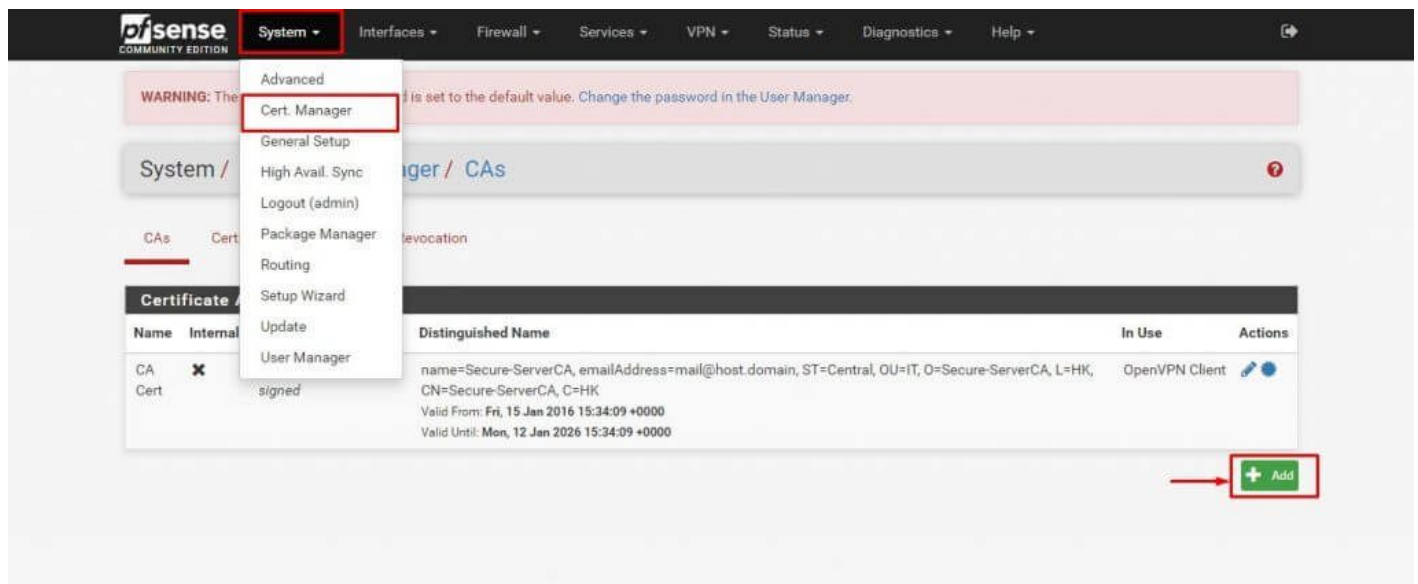
Things to Consider:

Before you begin, please make sure that you have:

- A working internet connection
- A VPN-supported router.
- A premium PureVPN account (If you do not already own one, you can buy a subscription from purevpn.com)

1 In order to configure OpenVPN on pfSense, first download the required OpenVPN Files from [here](#) and extract them.

2 After accessing your pfSense account, look for **Cert Manager** under **System** and click **+** to add a new certificate.



3 Now, input the following information:

- Descriptive name: Enter **CA Cert**
- Certificate data: After downloading the necessary OpenVPN files, copy its content from **Open CA2.crt** and paste it.
- Once done, click the **Save** button.

Create / Edit CA

Descriptive name

Method

Existing Certificate Authority

Certificate data

Certificate Private Key (optional)

Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

Serial for next certificate

Enter a decimal number to be used as the serial number for the next certificate to be created using this CA.

4 Select the **Certificates** tab and then click the **+** icon. Input the following information:

- Descriptive name: Enter **Client Cert**.
- Certificate data: After downloading the necessary OpenVPN files, copy its content from **Open Client.crt** and paste it.
- **Private key data**: From the downloaded OpenVPN files, access **Open Client.key**, copy its content and paste it.

Once done, click **Save**.

CA's Certificates Certificate Revocation

Add/Sign a New Certificate

Method Import an existing Certificate

Descriptive name

Import Certificate

Certificate data

```
-----BEGIN CERTIFICATE-----
MIIE6TCCA9GgAwIBAgIBAJANBgkqhkiG9w0BAQFADCBkTElMakGA1
UEBhMCEsEs
CzA7BgWVBAgTAKhLHREvDwYDQCEwIhIb25n529uZzEQMA4GA1UECh
MHUHVyZVZQ
-----
```

Paste a certificate in X.509 PEM format here.

Private key data

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQFAA5CBKggSkAgEAAoIBAQDN1Z
VpwhjGpIv
Gh+9zhBB911/z6XOR11cDk0cgz19Qpd6Hi8KiVrBapk9/HTNL+TmJ
RHR3L0MPkz
-----
```

Paste a private key in X.509 PEM format here.

Save

5 Select **VPN** and then choose **OpenVPN** from the drop-down menu.

System Interfaces Firewall Services **VPN** Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. Change the password in the System Manager.

System / Certificate Manager / CA's

CA's Certificates Certificate Revocation

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA Cert	✘	self-signed	0	name=Secure-ServerCA, emailAddress=mail@host.domain, ST=Central, OU=IT, O=Secure-ServerCA, L=HK, CN=Secure-ServerCA, C=HK Valid From: Fri, 15 Jan 2016 15:34:09 +0000 Valid Until: Mon, 12 Jan 2026 15:34:09 +0000	OpenVPN Client	

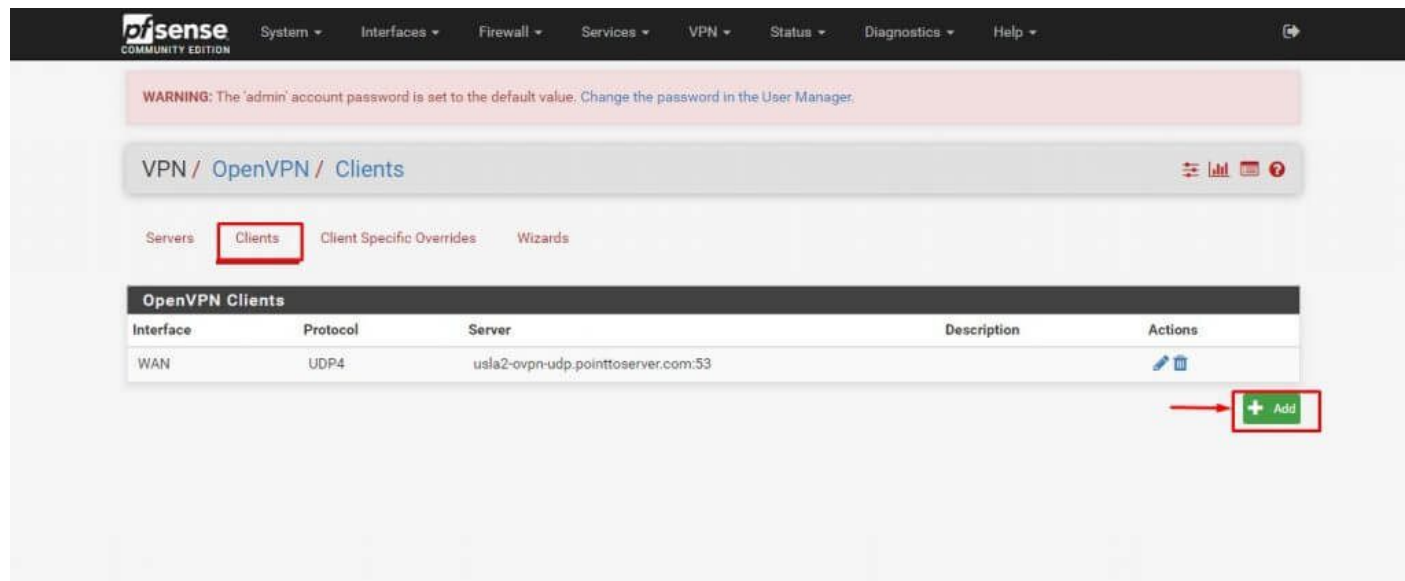
+ Add

6 Select the **Clients** tab and click the **+** icon.

PureVPN Support

Solution of Your Problems

<https://support.purevpn.com>



Next, input the following information:

- Server mode: **Peer-to-Peer (SSL/TLS)**
- Protocol: **UDP on IPv4 only** or **TCP on IPv4 only**
- Device mode: **Tun – Layer 3 Tunnel Mode**
- Interface: **WAN**
- Server host or address: Enter any OpenVPN server address, such as **usla2-ovpn-udp.pointtoserver.com**
- Server port: Depending on the protocol previously selected (**80** for **TCP** or **53** for **UDP**) select the appropriate port number
- User Authentication Settings: Enter your **PureVPN username and password**

Under Cryptographic settings, do the following:

- Check the **Use a TLS Key** box next to **TLS Configuration**
- Access **Open WDC.key**. Copy and paste its content in the next box
- TLS Key Usage Mode: Choose **TLS Authentication**
- Peer Certificate Authority: **CA Cert**
- Client Certificate: **Client Cert**
- Encryption Algorithm: **AES-256-CBC**
- Enable NCP: Check the **Enable Negotiable Cryptographic Parameters** box
- Auth digest algorithm: **SHA1 (160 bit)**
- Hardware Crypto: Set it to **No Hardware Crypto Acceleration**

Cryptographic Settings

TLS Configuration Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

TLS Key
d4283db4b48bcdda9c9e8759a3799d1c
793966a5989168c9668du8F6125c1b2f
585b41c874b2fe88ecfc-f17aab9a33be
1352379cdF74952b588fb161a99e13df
9135b2b29838231e@2d657a632578fe6-
Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.

TLS Key Usage Mode TLS Authentication
In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.

Peer Certificate Authority CA Cert
Peer Certificate Revocation List
No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager > Certificate Revocation](#)

Client Certificate Client Cert (In Use)

Encryption Algorithm AES-256-CBC (256 bit key, 128 bit block)
The Encryption Algorithm used for data channel packets when Negotiable Cryptographic Parameter (NCP) support is not available.

Enable NCP Enable Negotiable Cryptographic Parameters
Check this option to allow OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic Encryption Algorithms from those selected in the NCP Algorithms list below.

NCP Algorithms
Available NCP Encryption Algorithms
Click to add or remove an algorithm from the list
The order of the selected NCP Encryption Algorithms is respected by OpenVPN.
Allowed NCP Encryption Algorithms. Click an algorithm name to remove it from the list

Auth digest algorithm SHA1 (160-bit)
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present. When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel. Set this to the same value as the server. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto No Hardware Crypto Acceleration

Under Advanced Settings, do the following:

- Gateway Creation: **IPv4 only**
- Click the **Save** button.

Advanced Configuration

Custom options

Enter any additional options to add to the OpenVPN client configuration here, separated by semicolon.

UDP Fast I/O Use fast I/O operations with UDP writes to tun/tap. Experimental.
Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.

Send/Receive Buffer

Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.


Gateway creation Both IPv4 only IPv6 only

If you assign a virtual interface to this OpenVPN client, this setting controls which gateway types will be created. The default setting is 'both'.

Verbosity level

Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

None: Only fatal errors
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range




7 Under **Firewall**, click **NAT**.



Port Forward 1:1 **Outbound** NPt

Outbound NAT Mode

Mode	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
	Automatic outbound NAT rule generation. (IPsec passthrough included)	Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)	Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	Disable Outbound NAT rule generation. (No Outbound NAT rules)

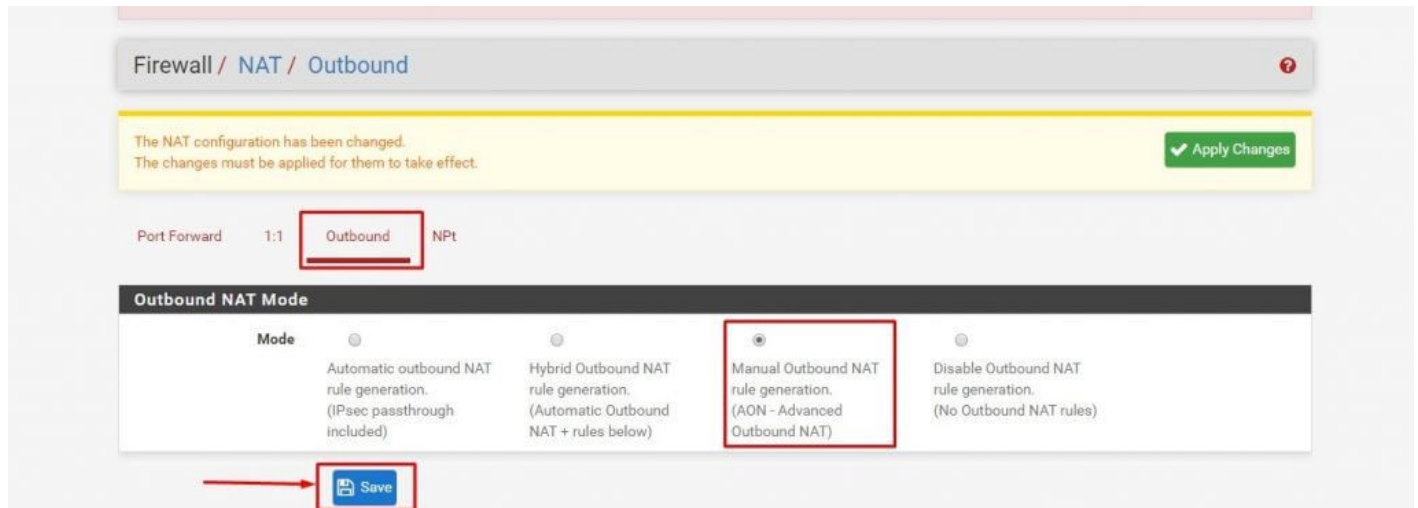


Mappings

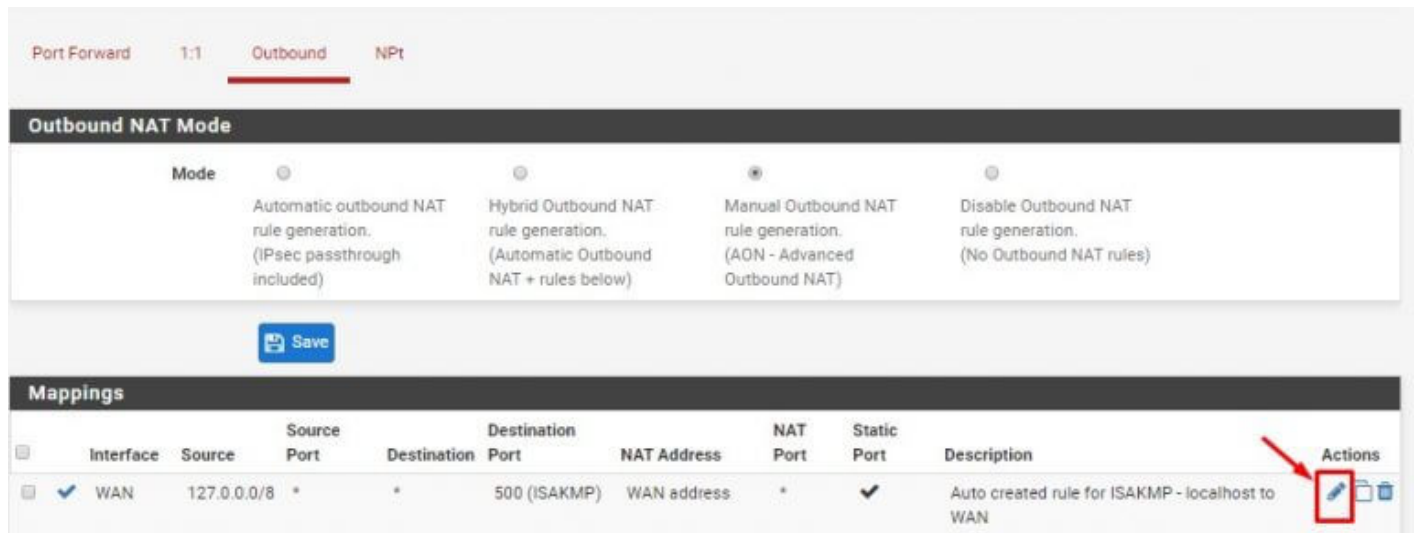
Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input checked="" type="checkbox"/> WAN	127.0.0.0/8	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - localhost to WAN	 

8 Select **Outbound** and then click **Manual Outbound NAT rule generation (AON Advanced**

Outbound NAT) under **Outbound NAT Mode**. Click **Save** to apply changes.



9 You will be presented with a mapping window. Each WAN perimeter within needs to be changed to OpenVPN. This can be done after clicking on the **Edit** button.



10 **Interface** needs to be changed to **OpenVPN**. Click **Save**.

Firewall / NAT / Outbound / Edit

Edit Advanced Outbound NAT Entry

Disabled Disable this rule

Do not NAT Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules
 In most cases this option is not required.

Interface WAN This is "WAN" or another externally-connected interface.

Address Family IPv4+IPv6

Protocol any Choose which protocol this rule should match. In most cases "any" is specified.

Source Network 127.0.0.0 / 8 Source network for the outbound NAT mapping. Port or Range

Destination Any / 24 500 Destination network for the outbound NAT mapping. Port or Range

Not Invert the sense of the destination match.

11 The above mentioned step is repeated 3 time across the board for all interfaces to OpenVPN, after which the mapping window will look something like the image below.

Port Forward 1:1 **Outbound** NAT

Outbound NAT Mode

Automatic outbound NAT rule generation. (IPsec passthrough included)

Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)

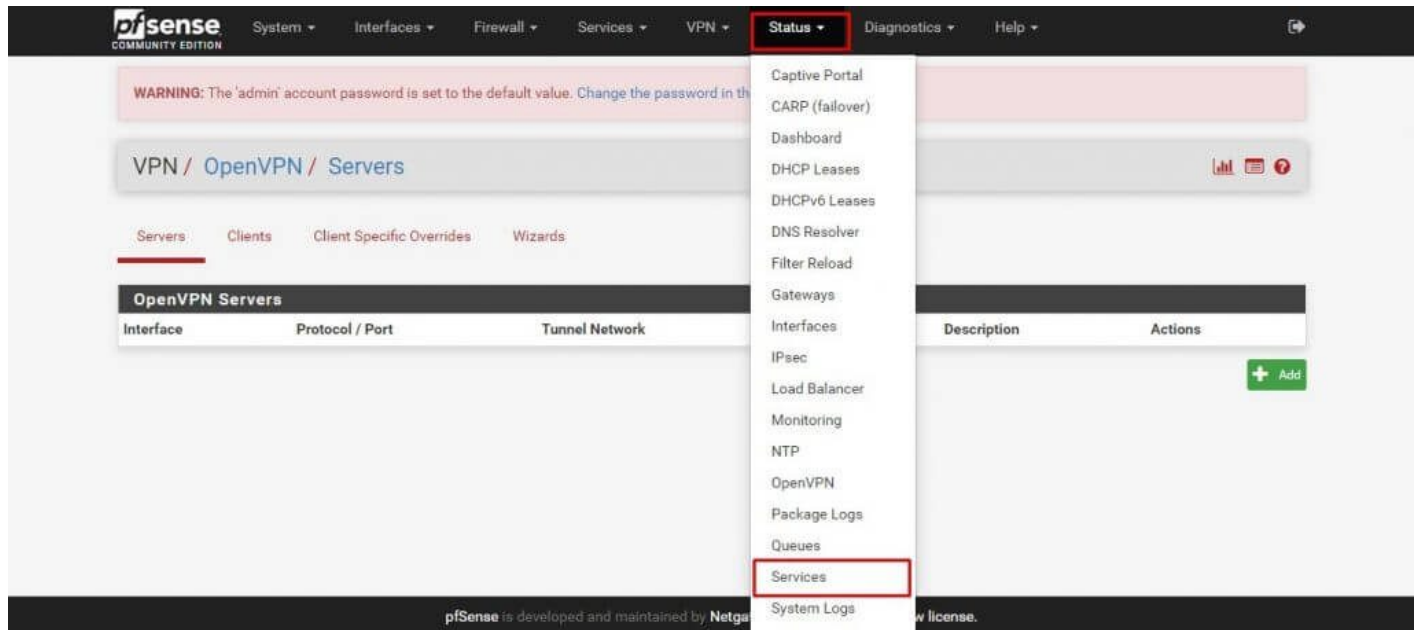
Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)

Disable Outbound NAT rule generation. (No Outbound NAT rules)

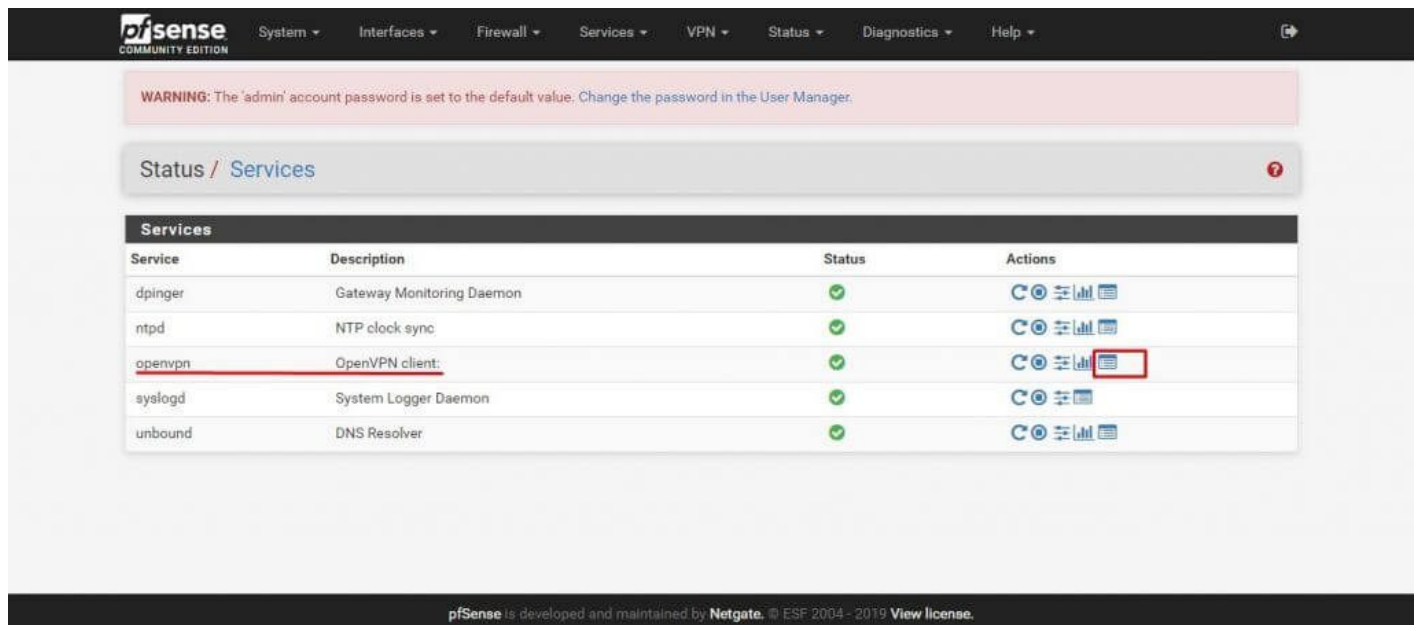
Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input checked="" type="checkbox"/> OpenVPN	127.0.0.0/8	*	*	500 (ISAKMP)	OpenVPN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - localhost to WAN	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input checked="" type="checkbox"/> OpenVPN	127.0.0.0/8	*	*	*	OpenVPN address	*	<input checked="" type="checkbox"/>	Auto created rule - localhost to WAN	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input checked="" type="checkbox"/> OpenVPN	::1/128	*	*	500 (ISAKMP)	OpenVPN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - localhost to WAN	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input checked="" type="checkbox"/> OpenVPN	::1/128	*	*	*	OpenVPN address	*	<input checked="" type="checkbox"/>	Auto created rule - localhost to WAN	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

12 Click **Services** under **Status**.



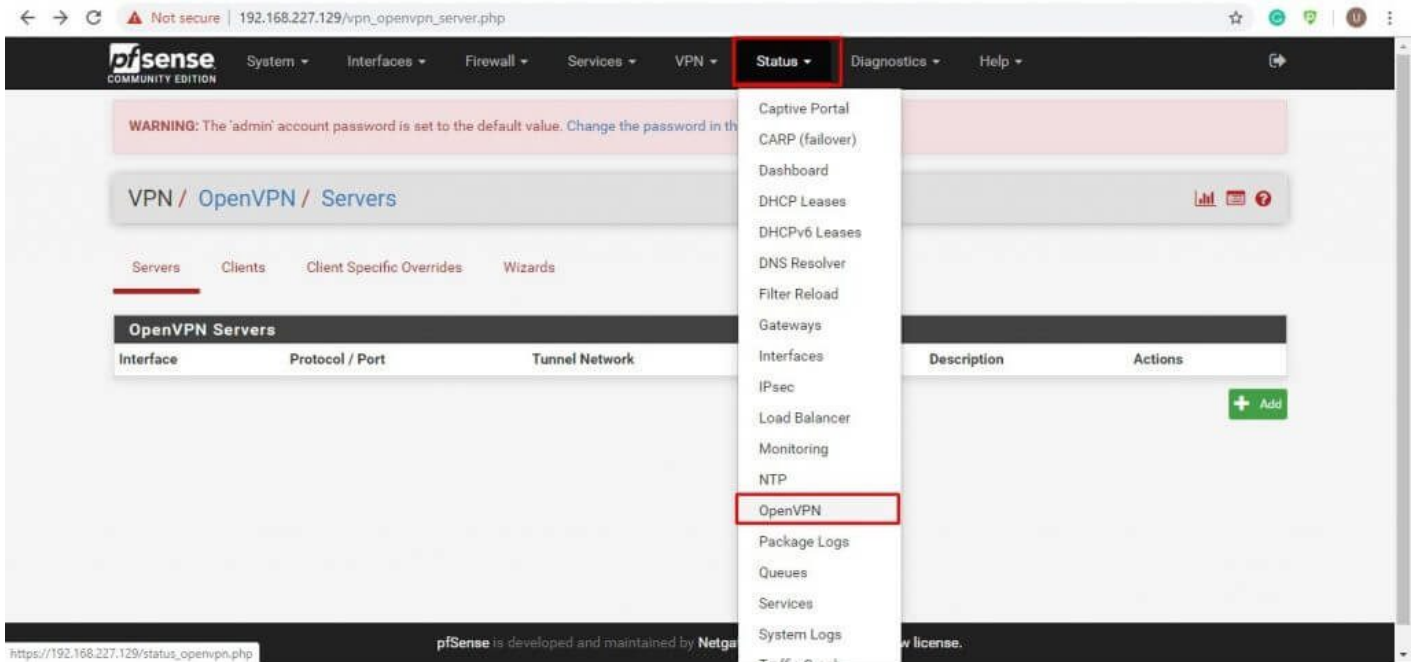
13 To access OpenVPN client, click **Log Entries**.



14 Once initialization is complete for the logs, it will confirm your connection.

Dec 9 13:01:32	openvpn	32380	SIGUSR1[soft:ping-restart] received, process restarting
Dec 9 13:01:32	openvpn	32380	Restart pause, 10 second(s)
Dec 9 13:01:42	openvpn	32380	NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
Dec 9 13:01:42	openvpn	32380	TCP/UDP: Preserving recently used remote address: [AF_INET]172.111.147.4:1194
Dec 9 13:01:42	openvpn	32380	Socket Buffers: R=[42080->42080] S=[57344->57344]
Dec 9 13:01:42	openvpn	32380	UDPv4 link local (bound): [AF_INET]192.168.227.129:0
Dec 9 13:01:42	openvpn	32380	UDPv4 link remote: [AF_INET]172.111.147.4:1194
Dec 9 13:26:18	openvpn	87630	WARNING: file '/var/etc/openvpn/client1.up' is group or others accessible
Dec 9 13:26:18	openvpn	87630	OpenVPN 2.4.6 amd64-ports-freebsd11.2 [SSL (OpenSSL)] [LZO] [LZ4] [MH/RECVDA] [AEAD] built on Oct 3 2018
Dec 9 13:26:18	openvpn	87630	library versions: OpenSSL 1.0.2o-freebsd 27 Mar 2018, LZD 2.10
Dec 9 13:26:18	openvpn	87969	WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.
Dec 9 13:26:18	openvpn	87969	NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
Dec 9 13:26:19	openvpn	87969	TCP/UDP: Preserving recently used remote address: [AF_INET]172.111.147.4:53
Dec 9 13:26:19	openvpn	87969	UDPv4 link local (bound): [AF_INET]192.168.227.129:0
Dec 9 13:26:19	openvpn	87969	UDPv4 link remote: [AF_INET]172.111.147.4:53
Dec 9 13:26:19	openvpn	87969	WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Dec 9 13:26:20	openvpn	87969	[Secure-Server] Peer Connection Initiated with [AF_INET]172.111.147.4:53
Dec 9 13:26:22	openvpn	87969	TUN/TAP device ovpn1 exists previously, keep at program end
Dec 9 13:26:22	openvpn	87969	TUN/TAP device /dev/tun1 opened
Dec 9 13:26:22	openvpn	87969	ioctl(TUNSIFMODE): Device busy (errno=16)
Dec 9 13:26:22	openvpn	87969	do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Dec 9 13:26:22	openvpn	87969	/sbin/ifconfig ovpn1 172.111.147.222 172.111.147.193 mtu 1500 netmask 255.255.255.192 up
Dec 9 13:26:22	openvpn	87969	/usr/local/sbin/ovpn-linkup ovpn1 1500 1558 172.111.147.222 255.255.255.192 init
Dec 9 13:26:22	openvpn	87969	Initialization Sequence Completed

15 You can check status of the VPN connection from **Status** under the **OpenVPN** tab.



Status / OpenVPN



Client Instance Statistics

Name	Status	Connected Since	Local Address	Virtual Address	Remote Host	Bytes Sent/Received	Service
Client UDP4	up	Mon Dec 9 13:26:22 2019	192.168.227.129/21151	172.111.147.222	172.111.147.4:53	79 KiB / 113 KiB	  